The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
02/12/2013

SUBJECT:
Multiple Vulnerabilities in Adobe Flash Player and Adobe AIR Could Allow Remote Code Execution (APSB13-05)

OVERVIEW:
Multiple security updates have been released for Adobe Flash Player and Adobe AIR. Adobe Flash Player and Adobe AIR are widely distributed multimedia and application players used to enhance the user experience when visiting web pages or reading email messages. Adobe Flash Player is prone to seventeen vulnerabilities that could allow for remote code execution or information disclosure.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

SYSTEMS AFFECTED:
- Adobe Flash Player 11.5.502.149 and earlier versions for Windows and Macintosh
- Adobe Flash Player 11.2.202.262 and earlier versions for Linux
- Adobe Flash Player 11.1.115.37 and earlier versions for Android 4.x
- Adobe Flash Player 11.1.111.32 and earlier versions for Android 3.x and 2.x
- Adobe AIR 3.5.0.1060 and earlier versions
- Adobe AIR 3.5.0.1060 SDK and earlier versions

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

Adobe Flash Player is prone to seventeen vulnerabilities that could allow for remote code execution or information disclosure. The vulnerabilities are as follows:

- Multiple buffer overflow vulnerabilities that could lead to code execution (CVE-2013-1372, CVE-2013-0645, CVE-2013-1373, CVE-2013-1369, CVE-2013-1370, CVE-2013-1366, CVE-2013-1365, CVE-2013-1368, CVE-2013-0642, CVE-2013-1367)
- Multiple use-after-free vulnerabilities that could lead to code execution (CVE-2013-0649, CVE-2013-1374, CVE-2013-0644)
- An integer overflow vulnerability that could lead to code execution (CVE-2013-0639)
- Multiple memory corruption vulnerabilities that could lead to code execution (CVE-2013-0638, CVE-2013-0647)
- A vulnerability that could result in information disclosure (CVE-2013-0637)

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Users of Adobe Flash Player 11.5.502.149 and earlier versions for Windows should update to Adobe Flash Player 11.6.602.168.
- Users of Adobe Flash Player 11.5.502.149 and earlier versions for Macintosh should update to Adobe Flash Player 11.6.602.167
- Users of Adobe Flash Player 11.2.202.262 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.270.
- Flash Player installed with Google Chrome will automatically be updated to the latest Google Chrome version, which will include Adobe Flash Player 11.6.602.167 for Windows, Macintosh and Linux.
- Flash Player installed with Internet Explorer 10 for Windows 8 will automatically be updated to the latest Internet Explorer 10 version, which will include Adobe Flash Player 11.6.602.167 for Windows.
- Users of Adobe Flash Player 11.1.115.37 and earlier versions on Android 4.x devices should update to Adobe Flash Player 11.1.115.47.

- Users of Adobe Flash Player 11.1.111.32 and earlier versions for Android 3.x and earlier versions should update to Flash Player 11.1.111.43.
- Users of Adobe AIR 3.5.0.1060 and earlier versions should update to Adobe AIR 3.6.0.597.
- Users of the Adobe AIR 3.5.0.1060 SDK (including AIR for iOS) and earlier should update to the new Adobe AIR 3.6.0.599 SDK + Compiler.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.

REFERENCES:

Adobe:

https://www.adobe.com/support/security/bulletins/apsb13-05.html

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1372
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0645
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1733
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1369
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1366
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0649
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1374
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1368
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0642
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0644
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0647
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1367
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0638
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0637